The materiality of virtuality

Loute, Alain; Grandjean, Nathalie

Published in:
(In)Disciplines

Publication date:
2019

Document Version
le PDF de l'éditeur

The materiality of virtuality: towards an intensification of invisibilities

"Forget about fingerprints or iris recognition; the way you walk or move your hands, even your pulse, can be analysed for unique characteristics. EU-funded researchers are looking at ways this new technology could protect your security and make identity checking less obtrusive and more accurate" [1].

Western societies face two paradoxical anxieties regarding political and social regulation: security and privacy. One of the polical choices of the European Union trying to solve this double bind resides in the promotion of technological solutions, such as 'soft biometrics'. Funding instruments such as 6th and 7th Framework Programmes promoted research in soft biometrics, following the objectives of robust identification while respecting privacy and bodily integrity. This new kind of biometrics shows great promise. As Dr Tzovaras says of the results of the ACTIBIO[2] project:

> (…) this is a revolutionary improvement for dynamic recognition. And when we combine dynamic and static biometric systems, the equal error rate drops to zero; identification is correct every time. We can see many excellent applications for authenticating individuals and monitoring their behaviours without having to intrude into or interrupt what they are doing"[3].

This non-intrusiveness is promoted as a technical quality which could render biometrical technologies harmless - indeed in some cases democratic - and therefore that could solve the famous "trade-off between security and privacy." Non-intrusive technologies are not only dedicated to biometric uses, but to any monitoring devices incorporating this quality of non-intrusiveness into their technological nature, for example when securing delimited critical infrastructures (CI), which is the objective of the P5[4] and IPATCH[5]. A new form of

---

[1] http://cordis.europa.eu/result/rcn/88445_en.html

[2] http://cordis.europa.eu/project/rcn/85410_en.html

[3] http://cordis.europa.eu/result/rcn/88445_en.html

[4]" "P5 project is the acronym of" "Privacy Preserving Perimeter Protection Project"" and is a European and FP7 funded project for the protection of critical infrastructures to benefit the sustainability of society and future well-being of European Citizens. Our vision is an intelligent perimeter proactive surveillance system that works robustly under a wide range of weather and lighting conditions. The system will monitor the region outside the security area of critical buildings and infrastructures, and give an early warning if terrestrial or airborne threats are approaching. The envisioned system will support, rather than replace, a human operator. A low false alarm rate from animals or other innocuous events, combined with high threat detection sensitivity and privacy

surveillance could emerge, lighter and less agressive. The walls become invisible. As underlined by Frank Neisse and Alexandra Novosseloff:

> "(…) first made of continuous obstacles of concrete or steel at regular intervals, of observation towers, walls progressively incorporate multiple electronic detection equipment. In the United States, drones equipped with infrared cameras now fly regularly along parts of the border. 30-meter-high observation towers have been installed in desert areas: there are soaring metal pylons on which are fixed cameras and radars able of covering 45 kilometers of border. This electronic ensemble constitutes thus a kind of "invisible wall" which will detect nearly 95% of migrants, according to the Border Patrol. This virtual wall, costing an exorbitant amount, has the great advantage of being more "acceptable" in the eyes of the people concerned, because it is less visible and, apparently, less violent." (Neisse & Novosseloff, 2010 :736)

The wish of the EU, through the funding of such research, resides in the idea that some political and social issues will be resolved through the possibility of creating virtuous technologies, both respectful of fundamental rights and privacy and yet effective for their monitoring objectives. Thus, the search produced PET (Privacy Enhancing Technologies) and the concept of 'Privacy by Design[6],' inaugurated by Ann Cavoukian, has emerged in the research and development sector. By integrating constraints of privacy at the heart of the construction of technological artefacts, one entrusts to technologies the power to solve the social, political and legal issues caused previously by the uses of surveillance.

---

standards, are central ambitions of the project."" http://www.foi.se/en/Customer--Partners/Projects/P5/P51/

[5] IPATCH (Intelligent Piracy Avoidance using Threat detection and Countermeasure Heuristics) is also a European and FP7 funded project, whose objectives are the detection of piracy threats in good time in high-risk areas. "IPATCH will provide technology to protect ships and their crews from the modern-day scourge of piracy that is proliferating throughout the world, bringing severe human, financial and political costs, as well as affecting international seaborne trade. The IPATCH system will use advanced sensors and data fusion to provide the Master of the ship with the information needed to decide how best to mitigate the threat, be that calling for assistance or bringing the crew into the secure citadel." http://www.ipatchproject.eu/

[6] "In the early 1990s, the concept of Privacy by Design (PbD) was developed to address the systemic effects of ICT and networked data systems. The central thesis of PbD is that privacy cannot be protected solely through compliance with regulatory instruments; rather, technologies should be designed with privacy in mind from the outset. Instead of bolting on privacy enhancing features, privacy enhancing tools e.g. minimisation of unnecessary data collection, should be integrated into systems design" (European Group on Ethics in Science and New Technologies, Jim Dratwa (ed.) ," "Ethics of Security and Surveillance Technologies", Opinion n° 28, (2014): 32. For a presentation of the 7 Fundamental Principles of the privacy by design approach; Cavoukian, Ann, *Privacy by design, The 7 Foundational Principles*, https://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

One of the recogniseable attributes of all these surveillance technologies[7] is their non-intrusiveness, which we prefer to designate as virtuality. They are promoted as less invasive to the extent that their control is not "material", that is to say that surveillance is not always palpable in material terms, nor physically felt. Surveillance, in this process of 'invisibilisation', should alleviate the unpleasant weight of social control, while being extremely effective. Virtuality could then be seen as a softening of control: a kind of nonviolent surveillance, but efficient and certain. However, this is not the case. Indeed, this phenomenon of the "virtualization" of surveillance is more an extension and intensification of surveillance power. More materiality must be considered for this virtualization, since it is intended to serve as a form of political management of specific spaces (such as borders or urban areas) and human bodies (which we may designate with the foucaldian term of 'biopolitics').

Meanings of virtualisation in monitored spaces

In his book on the political history of barbed wire, Olivier Razac (2009) emphasizes five basic features of virtualisation of spatial boundaries. Although his analysis applies mainly to barbed wire (which represents a milestone in this history of virtualisation), it suggests that virtualization of technologies is as much in evidence in their use of lightweight material as in their frightening effectiveness. Between the old barbed wire and virtual walls made of new surveillance technologies, only the material has changed.
What exactly are the meanings of virtualisation, according to Razac?

- Virtualization means first *material erasure*. We could hit a brick wall, a virtual wall is intangible.
- In addition, relief from material allows a *gain in mobility*. While a fortress wall is difficult to build, barbed wire walls are installed with great ease and without significant costs.
- Such a mobility allows high *flexibility*. Rather than a delimitation of fixed and definitive spaces, a virtual wall can follow movements and flows. Unlike the stone, "the metal wire is a tensile material that bends under the action of an external force. This deformation action has the effect of absorbing the energy impact and increasing the resistance of the wire. (...) Flexibility and mobility combine in order to allow the absorption of aggression, the agressor is entrapped and gradually weakened."(Razac 2009: 150).
- Razac also highlights the discretion that a virtual boundary enables. Far from being a sign of weakness, the power of this type of delimitation lies in its discretion. It avoids frontal resistance and opposition.
- Finally, virtual boundaries are characterized by their reactivity. Barbed wire walls can slow down an attack and gain time to react. In addition, because any space in front of the wire can be monitored, a panoptic effect reinforces the feeling of being monitored and potentially deters crossing the virtual wall.

[7] David Lyon defines surveillance as "any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered" David Lyon, *Surveillance Society: Monitoring Everyday Life* (Oxford: Open, 2001), 2.

Olivier Razac defines the concept of virtualisation of spatial boundaries from the study of a relatively low-tech device: barbed wire. It is therefore not necessary to mobilize digitised surveillance technologies as determining causes to understand this phenomenon of "virtualisation". On the contrary, the sense of the role of these technologies should rather be interpreted with reference to this virtualisation process.

Virtuality as political management of space

How to understand what is crucially at stake in this phenomenon of virtualisation? One must first avoid assimilating virtual to "less real." As Razac points out, "virtualisation does not mean less control of space, on the contrary, a relief from physical presence is made in an act of separation for the direct benefit of the authority's capacity to act " (Razac 2009: 159). One should understand virtualisation as a new form of "political management of space", rather than a de-politicisation of space. It is less control than opening and closing spaces in order to manage the flow of open spaces, "managing permeability." "Controlling population without curbing it", because the goal is not to "block, but to let circulate "(Razac 2009: 125). The main issue is to manage what Michel Lussault call "trans-spatiality" that is to say "the specific action of passing" (Lussault 2012: 71). This management of crossing and access is based on different protocols. Michel Lussault especially evokes the act of *spinning* or *queuing*, namely an analysis of the optimization of the queuing process. He also mentions *filtering*, which "grants access for the purposes of verification - usually the right to penetrate the space and/or content of what an individual or a container carries" (Lussault 2012: 71). Finally, the *tracing* process consists in "following an item entered into a spatial organization and at least identify its exit, better, its steps and its exit, better yet, all its movements and positions in a real-time process" (Lussault 2012: 72).

Even more than the passing or the crossing, the movement itself becomes the object of control and surveillance. So-called "smart" technologies can automatically detect behaviour considered as abnormal (or potentially abnormal): "it is possible to analyse behaviour considered as suspicious in open or public places: frequent stops, counterflow traffic, excessive or insufficient speed, group size, abandoned object, etc. with all the possible crosses between different chosen criteria"(Razac 2009: 220).

John Amos Lecat-Deschamps also considers videosurveillance as virtual walls (Lecat-Deschamps 2012: 124-9). The cameras are indeed sparsely visible in public space. On the opposite of the physical wall, CCTV do not try to "block", they "do not create any immediate physical consequence". They track and analyze flow. Similarly, they have a panoptical deterrent effect. Individuals know they are seen, interiorizing somehow expected norms of behaviour in specific spaces.

Virtuality as virtue

Let's go further in exploring this virtuality. In the paper "Border work: surveillant assemblages, virtual fences, and tactical countermedia", Tamar Vukov and Mimi Sheller point

out the proximity between the words “virtuality” and “virtue”: “Virtuality also carries connotations of “virtue” - the virtue of borders, the virtuous traveler, the good passenger versus the unvirtuous, the cheater, the stowaway and the smuggler” (Vukov & Sheller 2013: 225-241). This proximity raises different questions: is it possible to propound a fixed, neutral and objective definition of a normal behaviour? Or is it possible to consider “normality” as a temporal and socially-embedded phenomenon? By classifying the behaviour of moving object as innocuous or as potential threats, virtual fences could define certain kinds of behaviour as virtuous.

For Ajana, “Governments and companies often promote the illusion that algorithmic processes and data-driven systems are purged from human bias and interference leading to more neutral, objective and automated decisions that are devoid of discrimination on the basis of race, ethnicity etc.”. However, according to Ajana, such a belief needs to be interrogated. She quotes Dwork and Mulligan: “Both the datasets and the algorithms reflect choices, among others, about data, connections, inferences, interpretation, and thresholds for inclusion that advance a specific purpose [...] classification systems are neither neutral nor objective, but are biased toward their purposes. They reflect the explicit and implicit values of their designers” (Dwork & Mulligan 2013).

The virtue of technologies pretends to stay in a so-called neutrality of values, because of of the objectivity of the technological devices. But no technology has never been neutral or deprived of values. In reality, biometrical technologies valorize some norms and behaviours by accepting them or by refusing others, such as smart CCTV programmed to detect abnormal behaviours. This process of sorting contributes to normalized norms and behaviours and to the perception of acceptable body types, movements and behaviours.

Virtuality as virtuosity

Tamar Vukov and Mimi Sheller also point out the semantic proximity between “virtuality” and “virtuosity”: “So on entering the virtual border space of the airport one becomes not only a virtual passenger (shadowed by the ‘‘data double’’, a kind of informational penumbra), but also a virtuous passenger (performing virtue and virtuosity)” (Vukov & Sheller 2013: 225-241).

This second proximity raises a second issue. “Virtual fences” not only monitor a perimeter, they can also “perform” it. Virtual fences do not only detect moving objects, they could also affect these objects. People walking around a monitored perimeter could adjust, with virtuosity, their behaviour to the mechanism of surveillance. Human beings are very specific “moving objects”. They are “reflexive moving objects”. Virtuosity becomes a necessary quality in order to pass borders and cross areas. Surveillance technologies contribute to the social sorting process, when distinguishing individuals according to their virtuosity to pass borders and to move through spaces. They reactivate domination criteria such as class, race and gender. Virtuosity is the ability to transcend or even to cheat with those criteria.

Etienne Balibar points out the "multiple meanings" of borders. Meanings of borders change according the direction of crossing or according to who crosses, whether a businessman or an unemployed male youth of immigrant origin. “In this latter case, a border becomes almost two distinct entities, which have nothing in common but a *name*. Today's borders (though in reality this has long been the case) are, to some extent, designed to perform precisely this task: not merely to give individuals from different social classes different experiences of the law, the civil administration, the police and elementary rights, such as the freedom of circulation and freedom of enterprise, but actively to *differentiate* between individuals in terms of social class” (Balibar 2002 : 81-82).

Virtuality as potentiality

Virtual fences do not only extend the object of surveillance from a spatial point of view, but also from a temporal point of view. The future is also monitored. Early warning system try to detected “potential” threatening behaviours. Monitoring the future raises both epistemological and ethical issues. In R&D projects, the future is envisaged from "projected scenarios" selected by the engineers. It is essential to not confuse these scenarios with reality itself. By definition, the future is not exhaustively foreseeable. We always select and prioritize potentiality, we choose some scenarios over others. Our relation to the future is framed by an “economy of attention” (Balibar 2002 : 81-82).

For Didier Bigo, the risk today is that we deny this radical unpredictability of the future and pretend that we have the capacity “to read the future as if it were a “future perfect[8]”. As he says, “security technology professionals now want to reduce all these possible futures to just one; which is often the future of the worst case scenario. And it is this selected future that they read as a future perfect, as a future already fixed, a future they already know (…) [This] is the by-product of the existence of transnational guilds of professionals of (in)security who share the same view of the world to come” (Bigo & Delmas-Marty 2011).

Reading the future is not only a scientific and a technological task. It is also a political challenge. How to "democratize" this economy of attention? Should we organize a collective deliberation on the "projected scenarios" selected in technological projects?

Virtuality and the political process of bordering

A last question concerns the political process of bordering. Virtual fences could deeply modify the way we understand political borders. To the question “what is a border?” Etienne Balibar responds that it is not possible to give a simple answer: “Basically because we cannot attribute to the border an essence which would be valid in all places and at all times, for all physical scales and time periods, and which would be perceived in the same way in all individual and collective experience“(Balibar 2002 : 81-82).

---

[8] In french: “un futur antérieur”, that is to say, literally, a *previous* future.

This theoretical complexity contrasts with the practical simplicity with which borders have been build. Balibar writes: “In other words, their practical definition requires a ‘reduction of complexity’, the application of a simplifying force”. Balibar adds: “the consequence has been that the borders within which the conditions for a relative democracy have in some cases been won, have themselves always been absolutely anti-democratic institutions, beyond the reach of any political purchase or practice”. That’s why it is important to be concerned with “what democratic control is exerted on the controllers of borders - that is to say, on states and supra-national institutions themselves”.

Therefore, virtualization of fences does not lead to a democratization of borders. On the contrary, we should admit the hypothesis that virtualization of surveillance implies a more difficult and complex democratisation of borders. One of the risks is that virtualization increases a high "social acceptability of borders", making them less visible and more discreet, without any democratic debate about their management.

Extension and intensification of surveillance

In conclusion, it seems essential to consider that virtualization does not mean a reduction of supervisory power, but is the exercise of a new materiality of this power, gaining a kind of *extension*. First, because its objective is not only to cross borders or boundaries, but also to move through space. Moreover, the extension of this power is not solely spatial, it is also temporal, because the purpose of these ‘smart’ devices is to detect illicit or abnormal behaviours - and even the supposed intention of repressible behaviour. As Btihaj Ajana writes, “the future, as such, is now gradually becoming a computing object made of speculative algorithmic probability” (Ajana 2015: 58-78).

Secondly, virtualization processes do not mean a de-realisation of walls and borders. It would be a mistake to understand the “virtualization of border" as a phenomenon implying the disappearance of the border or the limit. Virtualization does not make a fence less real. By contrast, a characteristic of virtual fences is that “bordering” is not made only by means that are “actual”, that is to say, embedded in materiality, but also with “virtual means”, in the sense of “potential”. By “potential means” should not be understood less real. By “potential means”, we understand means which are “actualized” when necessary - an example is a patrol that only intervenes when electronic sensors trigger an alarm (Razac 2009).

Moreover, virtual fences could be used in combination with a physical fence. Btihaj Ajana argues that virtual fences “augment the function and the intensity of borders“ (Ajana 2015: 58-78). Virtual fences can also create a purely virtual limit where it would not have been possible to build a wall for economic, technical or political reasons.

Finally, surveillance is interiorised and intensified. With this new configuration of panoptic power, individuals, knowing they are seen, tend to act in order to comply with the expected normal behaviour. this results in "mental barriers"(Lecat-Deschamps 2012) or "interiorised limits" (Sabot 2012). Olivier Razac, referencing Michel Lussault on this phenomenon, writes:

"the limits are often mental and immaterial, built into the spatial capital of each operator, and therefore their effects are powerful because they remain necessary even when no physical barriers are erected to organize spatiality" (Lussault 2007:198).

Virtualisation facing biopolitics

We showed that virtuality raises crucial ethical and political issues concerning the political management of space and temporality. What about individuals? How does this virtuality impact them?

A strong hypothesis might assume that the pervasiveness of surveillance technologies puts us in a permanent biometric regime, due to the possibility of aggregate data being constantly connected to one or more individuals. Can we imagine the virtualization of technologies actually passing through bodies? Digital surveillance technologies, including biometric technologies, also have the effect of "virtual tagging". They place us in a full biometric regime, to the extent that the collected and aggregated data can be connected to one or more individuals. Our lives are continuously measured, compared, profiled and/or evaluated.

This full biometric regime engenders biopolitics, in the sense that identifying, recognizing and monitoring the order of *life itself* (body or bodily parts) is biopolitical scheduling, much as public health policies target morbidity, birth or epidemics. This is about monitoring masses of bodies while being able to focus on a particular body, deviant, unwanted or dangerous, if the need arises.

Biometrics as a new biopolitics

Let us return to the foundations of biopolitics. In 1977, Michel Foucault defined biopower as a technique of power, acting through the matter of the body, "society's control over individuals is not only carried out through consciousness or ideology, but also through the body and with the body. The body is a bio-political reality; medicine is a bio-political strategy" (Foucault 2010 : 210).

Foucault thinks this political investment of bodies occurs on a double level, firstly on the individual level of singular existence and, secondly, in terms of the population, through political economy and the governance of social behaviour. He distinguishes on the one hand *anatomo-politics* as the study of strategies and practices by which power models individuals, from school to factory; monitoring and straightening individuals' bodies. Then, on the other, he distinguishes *biopolitics* as the political management of life, targeting not particular individuals, but entire populations; this involves managing health, hygiene, diet, sexuality and natality as political issues. In 1979, he wrote a summary of his lecture 'Birth of Biopolitics' and defined biopolitics as "the way we have tried, since the 18th century, to rationalize the problems posed to governmental practice by phenomena engendered through an ensemble of livings constituted as a population: health, hygiene, birth, life, race... "(Foucault 2010 : 818).

Let us focus on the genealogy of biometrics. Giorgio Agamben provides an early intuition. He compares biometrical practices to the political paradigm of the concentration camp, because of the tagging of bodies as a means of identification: "Thus, by applying to the citizen, or rather the human being as such, the techniques and devices invented for the dangerous

classes, States - which should be in the heart of politics – have transformed the citizen into the ‘usual suspect’, to the extent that humanity itself becomes a dangerous class. A few years ago, I wrote that the political paradigm of Western societies was not the City anymore, but the concentration camp, and that we had passed from Athens to Auschwitz. It was obviously a philosophical thesis, and not a historical narrative, because one should not confuse phenomena that should rather be distinguished. However, I would suggest that tattooing probably appeared in Auschwitz as the most natural and most economical way to manage the inscription and registration of the deported in concentration camps” (Agamben 2004).

Biometrics reactivates the figure of the concentration camp by rigorously identifying the living body with a person's identity, and making a passport from a physical detail. At the same time, biometrics performs this reactivation with an entirely new spirit: by rendering neutral and objective this naturalization of personal identity, and by simply designating it as convenient, useful, efficient and fast, biometrics can delete any infamous intention or degrading tagging. What was an infamous marking becomes a discrete recognition mode, which is difficult to oppose with notions of consent or consciousness. All the strength of biometrics lies in this "discretion", this virtual marking, almost invisible, almost impermanent compared to the logic of concentration camps and tattoos.

From Auschwitz to 9/11

However, we remain within a time of great infamy. Since 9/11, images of borders, migrants and terrorists have replaced those of concentration camps and Jews. Biopolitical practice is still relevant, though far from attaining saturation, in the sense that it overflows across the landscape of the society of control. Boundaries are the territory of post-9/11 biometrics: physical boundaries (sea walls, deserts, etc.) or intangible boundaries ("critical infrastructure", transit zones in airports).

Garapon and Foessel (2006) underlined that the generalization of biometrics finds its initial justification in the anonymity that characterises terrorist actions. It seems an appropriate and effective response to the fear of erasing traditionally accepted criteria for danger, such as nationality or religious affiliation. Biometrical parameters can identify any individual without knowing their national or community affiliation and according to criteria that owe nothing to his/her biography. And because of this kind of identification, biometrics allows the tracking of anything, such as monitoring the transport of goods on the principle of "traceability". The challenge is to identify individuals, to store their routes and to deduce a degree of danger from the nature of their observed movements.

Garapon and Foessel (2006) believed that ethnic, religious or racial considerations disappear with biometrics. We do not share this opinion: firstly, biometrics is now able to trace and digitize these criteria, and secondly, biometrics uses these criteria by superimposing them. However, any biographical or narrative consideration of race is effectively excluded: it is seen as pollution and noise.

As we have already mentioned, the symbol of the full biometric regime is the migrant. Migrants are exposed to the same biometrical biopolitics: bone tests, hairiness, teething tests, and genital tests are imposed in order to determine the real age of a person, declaring whether he/she is a minor. DNA tests are also conducted to establish the real kinship between two people seeking family reunification, and biometrical tests in order to verify the real identity of an individual ...

Biometrics is enrolled in a context where generalized surveillance becomes increasingly deterritorialized and intrusive, such as terrorism. Terrorism and biometric practices seem symetrical and become systemic. Terrorism, according to Garapon and Foessel, uses several strategies: firstly, that of individual indiscrimination and of confusion between private and public. Privileged spaces for the terrorist attack are what Marc Augé (1992) calls "non-places", places full of crowds but empty of subjects, such as airports, subways, train stations, shopping malls. Thus another terrorist strategy takes place: by targeting non-places, terrorism uses a "strategy of ubiquity": any place, provided it is full, is likely to become a battlefield.

"Non-places" are uninhabited, they are crossed by crowd flows, which are essentially anonymous because not recognized as ‘subjects’ of those places. The figure of the terrorist is built symetrically into this constraint: he/she also wants to be anonymous, invisible - in full enjoyment of the presumption of innocence typical of Western democracies. Thus he/she meets the norm of *verisimilitude*, the apparent normal stream of everyday life, until the actual trigger point of the terrorist act. Based on this ordinary and quotidian nature, the horror and unpredictability of the act and therefore its effects are increased, occuring in the vast forum of scandalous publicity, relayed by social media and *breaking news* TV shows. Garapon and Foessel use the term "delayed visibility" to describe this strategy. It is to counteract this strategy that biometrical systems think, anticipate, predict and understand terrorist intentions.

Biometrics is both a biopolitical practice and a set of techno-scientific products from research projects. The full biometric regime is a political choice, relying on the hope of a tipping point between the dissimulation and the visibility of a terrorist. This hope relies on identification criteria, stable because computerized, and encoded in a universal language, and permanent because registered in the permanence of the body.

It is thus the very materiality of the body, taken in the specific readability of the code, that enables a guarantee of identities and intentions. The intention here is not, in the sense that ‘Nature’ would comprehend them, a naturalization of the body, to assign and individuate. Indeed, bodies subjected to the full biometric regime are a construction, because they need to be read through a variety of biometric technologies. Nonetheless, a form of attachment to the 'naturality' of the body is demonstrated by the primordial nature of the flesh, without being embedded in any process of individuation. Citizens or subjects are not necessary here – what counts is only the materiality of their bodies.

(Human) bodies do not lie

There is an assertion of technoscientific and political truth: the body does not lie, although technology may indeed sometimes misread or hear badly. Faced with a radical and permanent uncertainty, the only possible and visible landmark is the truth of the body. But the truth of the body is enunciated by a neutral and universal technoscience, completely unaware of its privileged and dominant position[9]. These modes of veridiction appear normal and natural. This *a posteriori* naturalization of the physical evidence of the body also plays a role in the attachment to the distinctly 'biological' body, and therefore to the denial and rejection of any narrative or biographical possibility.

What is being played out, therefore, is a possible desubjection that occurs in the very design of biometrical artifacts. Facial Recognition of Emotions is a biometric technology capable of processing the expression of emotions in real-time. In this case, it is neither the emotions nor the feelings themselves that are identified, but only their expression, digitized by algorithms that are in turn derived from deterministic psychological models[10].

Another example are bodycams. These are small cameras attached to police uniforms, that police officers can snap on in the event of contentious situations. Here also, one can observe the conjunction of the body and the artifact producing a regime of truth. Neither the story of the marchers nor the story of the officer has value when compared to the "narrative" of video-footage hooked to the body.

Thus a strange regime of legitimacy is being established: the body is legitimate only if is depoliticised with regard to the state. Deprived of subjectivity and read as code, dignity only exists insofar as the observed object agrees to be reduced to a 'suffering body' or a 'humanitarian body'. This body then acquires rights, like little Francesca[11], in May 2015. The humanitarian body, starving in Africa, is granted the opportunity to obtain rights; but political

---

[9] Similarly, american feminists denounced the "male gaze" as a dominant and privileged position. Donna Haraway, among others feminists, compares the male gaze with the status of science when described as neutral, objective or universal. A kind of predation is exerted by the scientist who observes and produces scientific facts from nature.

[10] Paul Ekman is an american professor of psychology. Computerized models for the facial recognition of emotions, based on Ekman's work on the facial expression of emotions (with Friesen, Haggard and Isaacs), allow the improvement of surveillance technologies. See more about Paul Ekman; http://www.paulekman.com/paul-ekman/

[11] The Nigerian child, Francesca, was born May 4th, 2015, on a boat full of migrants. She touched Italy with her extraordinary birth by representing two biblical figures, Moses saved from the waters and Jesus, born in a stable, "poor among the poor." No doubt that she will receive Italian citizenship as a birth gift ... http://www.theguardian.com/world/2015/may/04/rescued-mediterranean-migrant-gives-birth-baby-girl-italian-navy-ship

or economic migrants arriving on Europe's borders are being escorted back, because they are undesirable once they have left their 'natural' habitat, Africa.

How to describe this bodily attachment embedded in the biometric system? It is biopolitical, inasmuch as it is a commitment to bodily materialities. However this body is dis-integrated, performing a non-integrity process, notably because of this attachment to bodily materialities through which biometric devices scan. The *lived or experienced body* is not convoked, because it is unable to provide a reliable basis for recognition, nor is the *physical body*, subject as it is to the vagaries of time and the possibility of concealment. Thus the biometric body is a paradox, insofar as it is both objectified (reduced to computer parameters) and natural (unalterable).

Speaking of *body attachment* is also taking the expression literally: what is the body tied, bound, connected to? These bodies are integrally attached to biometrical technologies and shaped in a systemic process of individuation, or *becoming*[12], through these technologies. Technologies shape bodies, despite us and with us; bodies and techonologies are engaged in a hermeneutical relationship that is yet to be written. This hybridity becomes primordial with regard to modes of existence of the body and challenges any ontological or naturalized primacy. No natural body pre-exists in a temporality that is thickened by digital intensification. The biometrical hybrid body is instantiated in a temporality that is understood as a 'future perfect' (cf. *supra*), with a non-narrative, because encoded, type of performativity.

[12] Becoming (*devenir*) is a concept coined by Deleuze and Guattari in "A Thousand Plateaus" (1980).

Conclusion

In this paper, we have demonstrated that digital virtuality, described in terms of non-intrusiveness or invisibility, cannot elude some very concrete material effects: there is an intensification and extension of the power of surveillance technologies, through the spatio-temporal organization of both borders and urban areas, and through the bodies of individuals. Biopolitics, as described by Foucault, takes a new face and encompasses new challenges. Surveillance technologies have shown their ability to intensify the power of sovereignty and disciplinary techniques. This is especially what Deleuze sensed when writing the "Postscript on the Societies of Control" in 1990, in which he described a world of surveillance and control written with a digital language, which would be the new regime of power, replacing the old disciplinary societies.

"In the societies of control … what is important is no longer either a signature or a number, but a code: the code is a *password*, while on the other hand, disciplinary societies are regulated by *watchwords* (as much from the point of view of integration as from that of resistance). The numerical language of control is made of codes that mark access to information, or reject it. We no longer find ourselves dealing with the mass/individual pair. Individuals have become *"dividuals,"* and masses, samples, data, markets, or *"banks"* (Deleuze 1992: 5).

Underlining the various regimes of power (sovereignty, disciplinary and control), Deleuze emphasizes the organic link existing between surveillance technologies and the very exercise of control. It is not an isomorphism but a co-generation between technologies, code as language, individuals and society.

"Types of machines are easily matched with each type of society -- not that machines are determining, but because they express those social forms capable of generating them and using them. The old societies of sovereignty made use of simple machines -- levers, pulleys, clocks; but the recent disciplinary societies equipped themselves with machines involving energy, with the passive danger of entropy and the active danger of sabotage; the societies of control operate with machines of a third type, computers, whose passive danger is crashing and whose active one is piracy or the introduction of viruses. This technological evolution represents, even more profoundly, a mutation of capitalism (…)" (Deleuze 1992: 6).

How can one withstand virtualization and its effects? A technical answer is proposed through conceptual tools such as Privacy by Design, which is "an approach to protecting privacy by embedding it into the design specifications of technologies, business practices, and physical infrastructures. That means building in privacy up front – right into the design specifications and architecture of new systems and processes[13]". This proposal incorporates the promises of the field of genetics and gene therapy, which would have us believe that once privacy is

[13] https://www.ipc.on.ca/english/privacy/introduction-to-pbd/

enshrined in DNA technology, it will no longer produce counter-privacy effects. In other words, once "vaccinated", technologies revert to a natural state of neutrality.

This technological solution is coupled with ethical and legal responses, as illustrated for example by the recommendations of the *The European Group on Ethics in Science and New Technologies* (EGE) in a recent opinion (Dratwa 2014: 32). This group advocates notably for the application of the principle of accountability, as it argues that "Privacy Impact Assessment procedures must form part of regulatory practice in Member States when new or modified information systems which process personal data are being introduced to the market". And as the UK Information Commissioner's Office[14] says: "Privacy Impact Assessments (PIAs) are an integral part of taking a *privacy by design* approach. (…) Privacy Impact Assessments are a tool that you can use to identify and reduce the privacy risks of your projects. A PIA can reduce the risks of harm to individuals through the misuse of their personal information. It can also help you to design more efficient and effective processes for handling personal data[15]."

These legal-technical responses certainly possess the virtue of paying attention to ethical and legal issues. The different actors engaged in the birth of these technologies try to moralize these technologies inside their mode of production. However, we wonder if these initiatives allow us to assess and respond to the material effects induced by these new forms of the virtualization of control and surveillance? How to measure and evaluate the impact of these forms of political management of space, temporality and bodies? How to respond to the risk of de-subjectivation of the body induced by the management of "naturalized" bodies constructed by biometrical technologies? What are the consequences of the political management of virtual fences regarding the qualification or delineation of common and public spaces? These questions remain open.

[14] The UK's independent authority set up to uphold information rights in the public interest promoting openness by public bodies and data privacy for individuals. See https://ico.org.uk/

[15] https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/

Bibliography

Agamben, Giorgio, "Non au tatouage biométrique", Le Monde, 10th of January 2004 http://www.lemonde.fr/archives/article/2004/01/10/non-au-tatouage-biopolitique-par-giorgio-agamben_348677_1819218.html

Ajana, Btihaj, "Augmented borders: Big Data and the ethics of immigration control", Journal of Information, Communication and Ethics in Society 13/1 (2015): 58-78.

Balibar, Etienne. *Politics and the Other Scene*. New York & London: Verso, 2002.

Bigo, D. and Delmas-Marty, M. (2011) 'The State and Surveillance: Fear and Control', http://cle.ens-lyon.fr/anglais/the-state-and-surveillance-fear-and-control-131675.kjsp?RH=CDL_ANG100100#P4

Cavoukian, Ann, *Privacy by design, The 7 Foundational Principles*,

https://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

Deleuze, Gilles. "Postscript on the Societies of Control." October 59 (1992): 3-7.

Dratwa, Jim (ed.) "Ethics of Security and Surveillance Technologies", EGE Opinion n° 28, (2014) http://bookshop.europa.eu/en/ethics-of-security-and-surveillance-technologies-pbNJAJ14028/

Dwork, Cynthia and Mulligan, Deirdre, "It's Not Privacy, and It's Not Fair", Stanford Law Review Online, (2013) http://www.stanfordlawreview.org/online/privacy-and-big-data/its-not-privacy-and-its-not-fair

Fœssel, Michaël et Garapon, Antoine. "Biométrie: les nouvelles formes de l'identité", Esprit 2006/8 (2006): 165-172.

Foucault, Michel. *Dits et écrits II*. Paris: Gallimard, 2001.

Lecat-Deschamps, Jean-Amos. "La vidéosurveillance, un mur virtuel". Hermès, La Revue 63 (2012): 124-129.

Lussault, Michel, "Trans-spatialités urbaines", Hermès, La Revue 63 (2012): 67-74.

Lussault, Michel. *L'homme spatial*. Paris: Seuil, 2007.

Lyon, David. *Surveillance Society: Monitoring Everyday Life*. Oxford: Open, 2001.

Neisse, Franck and Novosseloff, Alexandra "L'expansion des murs: le reflet d'un monde fragmenté ?", Politique étrangère 4/2010 (2010): 731-742.

Razac, Olivier. Histoire politique du barbelé. Paris: Flammarion, 2009.

Razac, Olivier, “La matérialité de la surveillance électronique”, Déviance et société 37, (2013): 389-403.

Sabot, Philippe, “Une société sous contrôle ?”, Methodos (online) 12 (2012) http://methodos.revues.org/2941

Vukov, Tamara and Sheller, Mimi “Border work: surveillant assemblages, virtual fences, and tactical counter-media”, Social Semiotics 22/3 (2013): 225-241.